Department of Homeland Security Daily Open Source Infrastructure Report for 24 March 2006

Current Nationwide Threat Level is ELEVATED Significant Risk of Terrorist Attacks
For info click here
http://www.dhs.gov/

Daily Highlights

- CNET News reports that a laptop belonging to Fidelity Investments with information on almost 200,000 current and former Hewlett−Packard employees was stolen last week. (See item 11)
- The San Francisco Chronicle reports that a bomb threat on a BART train halted service between the East Bay and San Francisco; 20,000 passengers were delayed and no bomb was found. (See item 15)

DHS Daily Open Source Infrastructure Report *Fast Jump*

Production Industries: Energy; Chemical Industry and Hazardous Materials; Defense Industrial Base
Service Industries: Banking and Finance; Transportation and Border Security; Postal and Shipping
Sustenance and Health: Agriculture; Food; Water; Public Health
Federal and State: Government; Emergency Services
IT and Cyber: Information Technology and Telecommunications; Internet Alert Dashboard
Other: Commercial Facilities/Real Estate, Monument &Icons; General; DHS Daily Report Contact Information

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *March 23, Clarion Ledger (MS)* — **New nuclear plant may be ready by 2015.** A new nuclear reactor could be pumping out electricity in Mississippi within the next decade if the permitting process is completed in a timely manner, Entergy officials say. Entergy CEO Wayne Leonard said that the project could be completed by 2014 or 2015. Entergy is involved in the reactor development as part of NuStart Energy, a consortium of nearly a dozen energy companies. Jeffrey S. Merrifield, one of five commissioners of the Nuclear Regulatory Commission, said two other sites −− one in Illinois, the other in Virginia −− also are going through the permitting process and face a similar timeframe. He said the 103 nuclear plants operating in the U.S. are running at 90 percent capacity, compared with about 68 percent in 1998. To maintain the

current output, Merrifield said new plants would need to be ready to come on line in about 10 years. The agency is dealing with 11 applications that could result in 17 reactors, Merrifield said.
Source: http://www.clarionledger.com/apps/pbcs.dll/article?AID=/20060323/BIZ/603230376/1005/biz

2. *March 23, Associated Press* — **Pipe corrosion biggest threat as Alaska marks Exxon Valdez spill.** Since the Exxon Valdez caused the worst oil spill in the nation's history, tankers that ship Alaska's crude oil to the West Coast have become stronger, with double hulls and redundant operating systems for safety. With the 17th anniversary of the 11 million−gallon spill on Friday, March 25, some say the potential for oil spill disasters has shifted onshore. Some see corrosion in the aging oil supply system as a growing threat to the state's pipeline system, as evidenced by a leak on the North Slope this month. Transit lines generally have not been subjected to regulations as rigorous as the main line, although state regulatory officials say that could change because of the spill. The main pipeline will be 30 years old in 2007. As the oil fields of the North Slope decline, the quality of oil is also declining, meaning coarser and heavier crude is flowing down the pipe, causing stress on it.
Source: http://www.chron.com/disp/story.mpl/nation/3742707.html

3. *March 22, CALSTART* — **Pentagon ratcheting down petroleum use, costs.** In an effort to reduce the U.S. military's spending amid high fuel costs, the Pentagon is looking at wind, solar, geothermal, biofuel, hybrids and hydrogen fuel cells as new sources of energy, reports UPI. The Defense Department uses more than four times as much energy as all other government agencies combined, and accounts for almost all the government's petroleum consumption, according to the Department of Energy. One way the Navy tries to increase the fuel efficiency of its ships is using copper−containing coatings on hulls to decrease film buildup and drag in the water. The Navy has also developed an incentives program for ship fuel efficiency. A Defense Department memo from November 2005 outlined energy management goals for the military, which included reducing energy consumption in facilities by two percent per year. The Air Force has already gone beyond a 2013 target, using renewable sources for 11 percent of its electricity, according to Air Force spokesperson Nicole VanNatter, who indicated the Air Force leads the nation in purchasing renewable energy.
Source: http://www.calstart.org/info/newsnotes/nn_detail.php?id=8142

4. *March 22, Agence France−Presse* — **Qatar launches 2.6 billion−dollar Energy City.** Qatar has launched a 2.6 billion−dollar project to build Energy City that aims to attract more of the world's energy players to set up shop in the resource−rich Gulf emirate. Energy Minister Abdullah bin Hamad al−Attiya said the project is in line with the country's strategy to become "an energy capital and the world's foremost supplier of liquefied natural gas (LNG)." Attiya said Qatar plans to export 77 million tons a year of LNG by 2012 compared with the present 25 million tons. Attiya also said Qatar, which is a member of the Organization of the Petroleum Exporting Countries, will boost its oil production to 1.1 million barrels per day (bpd) by 2010 from the present level of 800,000 bpd. Oil giants Total and ExxonMobile are among the most active players in Qatar's oil and gas industries. In November, Qatar Petroleum and ExxonMobile launched a 14 billion−dollar project to build the world's largest LNG refinery that will supply the U.S. market.
Source: http://www.turkishpress.com/news.asp?id=114372

5. *March 21, Reuters* — **Exxon sees incremental refinery growth.** Exxon Mobil Corp. Chairman and Chief Executive Rex Tillerson said Wednesday, March 22, creeping refinery capacity expansion would keep up with growing U.S. demand for refined products without the need to build a new refinery. A new refinery has not been built in the United States since 1976. Last year, President George W. Bush encouraged companies to build new oil refineries on old military bases to meet growing demand for gasoline and diesel, but so far none have planned to do so. "We don't have any plans for a greenfield refinery in the U.S., primarily because we don't think there is a need for one," Tillerson said at the National Petrochemical and Refiners Association annual meeting in Salt Lake City, UT. Tillerson said U.S. refiners should be able to maintain the average annual two percent expansion in crude oil refining capacity to keep up with demand. U.S. markets will also rely on imports, he said. "We've been able to add two percent per year for the past 10 years and we would expect to continue to make those capacity additions," Tillerson said.
Source: http://news.yahoo.com/s/nm/20060321/bs_nm/energy_exxon_refin ery_dc_1

6. *March 21, Reuters* — **Shell EP buys Canada oil sands.** Royal Dutch Shell Plc said on Wednesday, March 22, its Shell EP Americas unit paid $400 million last month to buy 10 properties in northern Alberta, the highest price ever paid for Canadian oil sands leases. The Hague−based Royal Dutch Shell said its U.S. unit has formed a new company, SURE Northern Energy Ltd., to assess and exploit its new holdings, even though its 78−percent−owned Canadian unit, Shell Canada Ltd., is already a top investor in the oil−rich region of northern Alberta. It came as a surprise that Royal Dutch Shell would establish its first wholly owned investment in Canada's upstream oil industry. "The name never came up...It's bizarre...Is Shell going to compete with itself, or is this a way of not diluting its interest (with other investors)?" said Wilf Gobert, analyst at Peters & Co. in Calgary. SURE Northern will test new technologies to evaluate and potentially develop its new holdings and will begin drilling appraisal wells on the leases this year. Companies operating in the region now produce more than 1.1 million barrels a day and that's expected to climb to more than three million barrels a day by 2015.
Source: http://news.yahoo.com/s/nm/20060321/wl_canada_nm/canada_ener gy_shell_oilsands_col_4

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

7. *March 23, Aviation Week* — **Rising trend: Pursuit of nontraditional, defense−related IT business.** Northrop Grumman Corp. is ramping up its pursuit of nontraditional, defense−related information technology business, according to Sidney Fuchs, president of Northrop Grumman Information Technology's Civilian Agencies group. The company joins a growing list of defense−related firms trying to find growth outside the Pentagon's budget−crunched future.

"The nontraditional defense market is growing at a faster rate than the traditional defense market," Fuchs said. IT in general is seen as blowing past mature, constrained defense sectors like shipbuilding, and more attention is turning to newer, homeland needs.
Source: http://www.aviationnow.com/avnow/news/channel_netdefense_story.jsp?id=news/NOR03236.xml

8. *March 22, U.S. Department of Defense* — **Missile defense system ties many elements together.** The proposed U.S. ballistic missile defense system is intended to tie numerous independent elements into a sophisticated Web of protection, U.S. military officials said. The stated mission of the Missile Defense Agency is to field a layered missile defense system that integrates land−, sea−, and air−based missile defenses to protect the U.S. homeland, deployed troops, and America's friends and allies against all types of ballistic missiles in all phases of flight. In other words, the United States is working toward the ability to shoot down short−, medium−, and long−range ballistic missiles in their boost phase; during their mid−course flight, normally outside of the Earth's atmosphere; and as they descend toward their target. The system will incorporate a global array of sensors and radars, satellite tracking and surveillance; interceptors aboard ships at sea; ground−based interceptor missiles in underground silos; mobile−launch interceptors; and powerful lasers fixed to aircraft. The goal is to have several cracks at shooting down enemy missiles in various stages of flight, as well as to hedge against an accidental ballistic missile launch. Currently, the United States has a limited missile defense capability.
Source: http://www.defenselink.mil/news/Mar2006/20060322_4576.html

9. *March 22, Government Accountability Office* — **GAO−06−160: Defense Logistics: Several Factors Limited the Production and Installation of Army Truck Armor During Current Wartime Operations (Report).** In April 2005, the Government Accountability Office (GAO) reported on factors affecting the timely production of up−armored high−mobility multi−purpose wheeled vehicles (HMMWV) and add−on armor kits for HMMWVs, as well as other items critically needed by deployed forces during Operation Iraqi Freedom. Due to high interest by Congress and the public regarding vehicle armor, GAO initiated this subsequent engagement to examine issues affecting the production and installation of armor for medium and heavy trucks. The objectives were to (1) determine the extent to which truck armor was produced and installed to meet identified requirements, (2) identify what factors affected the time to provide truck armor, and (3) identify what actions the Department of Defense (DoD) and the Army have taken to improve the timely availability of truck armor. To address these objectives, GAO collected and analyzed supply data for medium and heavy tactical trucks used by Army forces. Expanding on one of its April 2005 recommendations, GAO is recommending that the Secretary of Defense direct the Army to establish a process to document and communicate all urgent wartime funding requirements for supplies and equipment when identified and the disposition of funding decisions. DoD concurred with the intent of the recommendation.
Highlights: http://www.gao.gov/highlights/d06160high.pdf
Source: http://www.gao.gov/cgi−bin/getrpt?GAO−06−160

[Return to top]

Banking and Finance Sector

10. *March 23, Finextra* — **PayPal to launch SMS payments service.** PayPal has confirmed that it is launching a new mobile payments service that will allow its customers to make purchases and transfer funds using SMS text messages. The eBay subsidiary will launch its m−payments service in the next couple of weeks in the U.S., Canada, and the UK. PayPal spokesperson Sara Bettencourt said the firm currently has no specific plans to extend the service to the other 55+ countries where PayPal operates. The new service will allow registered users to use their Web−enabled phones to make person−to−person fund transfers or pay for purchases. Customers can make payments using a text message service or by calling an automated customer service system and using voice commands to transfer funds. The 'Text to Buy' service will also feature a facility for customers to purchase advertised items by sending a text message containing a product code located in the ad. Customers then receive an automated call asking them to confirm the order and to enter their mobile PIN. Users are then asked to confirm the delivery address. Purchases will be debited to PayPal accounts.
Source: http://www.finextra.com/fullstory.asp?id=15091

11. *March 23, CNET News* — **Laptop with Hewlett−Packard employee data stolen.** A laptop with information on almost 200,000 current and former Hewlett−Packard (HP) employees was stolen last week, putting them at risk of identity fraud. The stolen computer belongs to Fidelity Investments, which provides services to HP. The laptop was being used by several Fidelity employees in an off−site location, said Anne Crowley, a spokesperson for Fidelity. The data includes names, addresses, Social Security numbers, dates of birth, and other employment−related information, but not the personal identification numbers required to log on to Fidelity services, she said. Fidelity has reported the theft to law enforcement agencies and the matter is under investigation, Crowley said. There is no evidence that the information has been misused, she said. The information requires a special application, which expired a day or so after the laptop was stolen. Crowley said, "The data would be difficult to interpret and generally difficult to read or use."
Source: http://www.zdnetasia.com/news/security/0,39044215,39345372,0 0.htm

12. *March 22, Reuters* — **Malaysia central bank plugs money laundering loopholes.** Malaysia will sign a pact with China's central bank this year to share information to fight money−laundering, terror financing, and other crimes, the southeast Asian nation's central bank said on Wednesday, March 22. Malaysia has also signed similar pacts with financial intelligence authorities in Australia, Indonesia, the Philippines, and Thailand, according to the bank's annual report. The central bank said it had launched a review of domestic non−profit organizations to identify flaws that might allow them to be exploited as channels for money−laundering.
Source: http://asia.news.yahoo.com/060322/3/2hrqq.html

13. *March 22, Computerworld* — **Hackers use Trojan to target bank customers in three countries.** Hackers have for several weeks been quietly infecting hundreds of thousands of computers worldwide with a particularly sophisticated Trojan horse program designed to steal bank account information and other sensitive data from compromised systems, according to security researchers. The attacks have been largely targeted at stealing passwords, personal ID numbers, and other information of customers of several large banks in the United Kingdom, Spain, and Germany. “This is one of those big, under−the−radar threats that we’ve been

concerned about" for some time, said Ken Dunham of VerSign Inc. According to Dunham, hackers have been sending out hundreds of thousands of e−mails prompting users in those three countries to visit malicious Websites that use a Windows Metafile (WMF) exploit to download a Trojan program called MetaFisher on a victim's computer. The Trojan, which is also known as Spy−Agent and PWS, is then used to collect and send bank account and personal information from the compromised system to remote servers where the data is harvested. What sets MetaFisher apart from the hundreds of other similar Trojan programs is the sophistication of the command−and−control servers used to control it, said Eric Sites of Sunbelt Software Inc.
Source: http://www.computerworld.com/securitytopics/security/story/0 ,10801,109803,00.html

[Return to top]

Transportation and Border Security Sector

14. *March 23, Globe and Mail (Canada)* — **Amtrak fast−tracks passport rules.** New passport rules for Canadians traveling to the U.S. seem to have kicked in early at Amtrak. The rail service now requires passengers to provide passport numbers and expiry dates before buying tickets. The Western Hemisphere Travel Initiative −− legislation setting out rules for U.S. entry −− officially takes effect at the end of this year for sea and air travel, and on December 31, 2007 for border crossings on land. But according to Amtrak spokesperson Cliff Black, the application of existing rules has nonetheless been tightened up, so that the future laws are for all intents and purposes already in place. U.S. Customs and Border Protection has urged Amtrak to start requesting passports, Black said. And Amtrak is taking this request seriously, to the point that Canadian travellers crossing into the States from Vancouver, Montreal or Toronto are required to provide passport information before being permitted to purchase train tickets.
Source: http://www.theglobeandmail.com/servlet/story/RTGAM.20060321. wxamtrak0322/BNStory/specialTravel

15. *March 23, San Francisco Chronicle* — **Bomb threat delays San Francisco commuter trains.** Passengers on BART Wednesday, March 22, were evacuated during rush hour from the West Oakland station because of a bomb threat on one of the trains. All service between the East Bay and San Francisco was halted and about 20,000 passengers were delayed. The station was evacuated while BART police and bomb−sniffing dogs checked a westbound train and found nothing. The shutdown was ordered shortly after a passenger heard two men on the platform yelling that there was a bomb aboard a train that was just leaving for San Francisco, Johnson said. The passenger told the station agent, who immediately relayed the threat to BART police. Most of the 61−train fleet was delayed by the transbay bottleneck. It was the second time in two weeks that transbay service was halted during the morning commute. On March 9, a debris fire on the underground tracks near the Embarcadero station forced evacuation of that station, delayed tens of thousands of passengers.
Source: http://www.sfgate.com/cgi−bin/article.cgi?f=/c/a/2006/03/23/ BAGL1HSODD1.DTL

16. *March 22, Transportation Security Administration* — **TSA revokes certification for J.H. World Express for security violations at LAX.** The Transportation Security Administration (TSA) on Tuesday, March 22, announced that J.H. World Express, Inc. does not meet security standards and will have its indirect air carrier certification revoked for shipments on passenger aircraft. TSA Administrator Kip Hawley said, "As freight forwarders these agents are trusted to

maintain robust security, and comply with known shipper and other program requirements. When that responsibility is not met we will take action." During the past several months, TSA conducted numerous compliance inspections at the cargo facility of J.H. World Express, Inc. and found repeat, multiple violations. The last company to face a revoked certification by TSA was U.S. European Trading Inc. in Cape Coral, FL, in November, 2002.
Source: http://www.tsa.gov/public/display?theme=44&content=090005198 01bbc3b

17. *March 22, Associated Press* — **Regional jet with landing gear problem lands safely.** A Continental Express flight safely made an emergency landing Wednesday, March 22, after losing a wheel on its landing gear at its origination point. Albany International Airport spokesperson Doug Myers said Flight 2314 was traveling from Newark, NJ to Albany, NY with 37 people on board when the crew noticed the problem at 6:20 p.m. EST. The jet landed at 6:59 p.m. EST. No one was injured.
Source: http://www.newsday.com/news/local/wire/newyork/ny−bc−ny−−eme rgencylanding0322mar22,0,4311764.story?coll=ny−region−apnewy ork

[Return to top]

Postal and Shipping Sector

18. *March 22, Maine Today* — **Postage stamps and money stolen in burglary.** Intruders broke into the East Wilton, ME, Post Office sometime overnight Monday, March 20, stealing stamps and cash in what may become a federal crime, according to Wilton Police Chief Wayne Gallant. The mail was not compromised. A U.S. Postal Service inspector is scheduled to be in Wilton and determine if the burglary will be pursued as a federal crime.
Source: http://morningsentinel.mainetoday.com/news/local/2559070.sht ml

[Return to top]

Agriculture Sector

19. *March 23, Food and Agriculture Organization* — **Mad cow disease on the wane worldwide.** Cases of bovine spongiform encephalopathy (BSE) or mad cow disease worldwide are declining, according to the United Nations Food and Agriculture Organization (FAO). They have been dropping at the rate of some 50 percent a year over the past three years, the FAO said Thursday, March 23. In 2005, just 474 animals died of BSE around the world, compared with 878 in 2004 and 1646 in 2003, and against a peak of several tens of thousands in 1992, according to figures collected by the World Animal Health Organization (OIE), with which FAO works closely.
Source: http://www.fao.org/newsroom/en/news/2006/1000258/index.html

20. *March 23, University of Exeter* — **Scientists a step closer to protecting world's most important crop.** Scientists at the University of Exeter have shown for the first time how the world's most destructive rice−killer hijacks its plant prey. In order to infect plants the fungus has to inject its proteins into the plant's own cells where they overcome the plant's defences allowing a full scale invasion by the fungus. Until now it's not been known how the fungus

delivers that weaponry, but researchers from Exeter's School of Biosciences have identified a single gene that appears to be important in the process. Rice is the world's most important food security crop and it is thought that by 2020 rice consumers in Asia alone will have increased by 1.2 billion, making the fight to secure the global rice harvest essential.
Source: http://www.exeter.ac.uk/news/ricecrop.shtml

[Return to top]

Food Sector

21. *March 23, Reuters* — **Thailand battles major outbreak of botulism.** Thailand flew 17 people infected by severe botulism to Bangkok on Thursday, March 23, while dozens more were being treated in rural hospitals after one of the world's worst outbreaks of the muscle−paralyzing disease. The 17, including 12 women and a young girl, were among 160 villagers who fell ill after eating contaminated bamboo shoots during a festival in the northern province of Nan. More than 100 are in hospital, including 42 who needed respirators after they became too weak to breathe on their own. Thai health officials believe the Nan outbreak was caused by improper canning of the bamboo shoots, which allowed the bacteria to survive and produce the deadly toxin.
Source: http://abcnews.go.com/Health/wireStory?id=1758935

22. *March 22, U.S. Department of Agriculture* — **U.S. Department of Agriculture to dispatch technical team to Japan.** U.S. Department of Agriculture (USDA) Secretary Mike Johanns Wednesday, March 22, announced a USDA technical team will meet with Japanese government officials on Tuesday, March 28, and Wednesday, March 29, to answer questions and press for the reopening of the Japanese market to U.S. beef. Johanns directed that a USDA technical team go to Japan after the Japanese government signaled a willingness to receive USDA experts. Japan reopened its market to U.S. beef on December 11, 2005 but halted U.S. beef imports on January 20, 2006 after receiving a shipment of U.S. beef that posed no food safety risk but did not meet the specifications of the U.S. export agreement with Japan.
Source: http://www.usda.gov/wps/portal/!ut/p/_s.7_0_A/7_0_1OB?contentidonly=true&contentid=2006/03/0099.xml

23. *March 18, Associated Press* — **Pill found in candy investigated as case of possible tampering.** A home day−care provider said she found a pill mixed in with candy, and one of the children she was caring for tested positive for opiates, the Salt Lake, UT, sheriff's office said. Sheriff's Sgt. Mike Morgan said the candy, Nestle Nerds, was purchased at the Smith's Food and Drug store in Herriman. Morgan said Nestle, Poison Control, and the FBI were advised of the incident. He said the Smith's store removed its remaining Nestles Nerds from its shelves.
Source: http://www.heraldextra.com/content/view/170858/4/

[Return to top]

Water Sector

24. *March 23, Arizona Republic* — **Water spills investigated.** Prompted by a string of accidental radioactive discharges, federal monitors said Wednesday, March 22, that they have formed a task force to investigate the spills at several power plants across the country. "It does appear that it's bang, bang, bang, one right after the other," Steve Klementowicz, a Nuclear Regulatory Commission senior health physicist, said of discharges of radioactive tritium−laced water at nuclear plants in Arizona, Illinois, and New York. Tritium, a byproduct of nuclear power generation, is a relatively weak source of radiation. But long−term exposure can increase the risks of cancer, miscarriages, and birth defects. It can be ingested or absorbed in human tissue. Klementowicz and other NRC officials said a task force of experts will evaluate the health effects of what has happened at at least five plants since December and possibly earlier incidents.
Additional information is available on the NRC Website:
http://www.nrc.gov/reactors/operating/ops−experience/grndwtr −contam−tritium.html
Source: http://www.azcentral.com/news/articles/0323nuke−taskforce032 3.html

[Return to top]

Public Health Sector

25. *March 23, Agence France−Presse* — **Girl dies of bird flu in Cambodia, seven other suspected cases.** A three−year−old girl has died of bird flu in Cambodia, initial tests showed, and seven other suspected cases have been reported in the first outbreak in the country in two years. The girl died Tuesday, March 21, in the capital Phnom Penh after falling ill in western Kompong Speu province, said Ly Sovann, director of the health ministry's infectious disease department. Samples from the dead girl and seven other people showing signs of the H5N1 virus are being tested, Ly Sovann said. Officials at the Pasteur Institute in Phnom Penh confirmed the bird flu death, the fifth in the country since 2003.
Source: http://news.yahoo.com/s/afp/20060323/hl_afp/healthflucambodi a_060323170622

26. *March 22, World Health Organization* — **Americas, South−East Asia and Western Pacific regions on track to reach tuberculosis control targets.** Three of the world's six regions are expected to achieve targets for tuberculosis (TB) control, according to a World Health Organization (WHO) report published Wednesday, March 22. The Region of the Americas and the South−East Asia and Western Pacific regions should reach targets set by the World Health Assembly, to detect 70 percent of TB cases and to successfully treat 85 percent of these cases by the end of 2005. The WHO report confirms that 26 countries had already met the targets a year ahead of time, two of them being the high TB burden countries of the Philippines and Viet Nam. The report also indicates that five other high−burden countries −– Cambodia, China, India, Indonesia and Myanmar −– should have reached the targets within the 2005 time frame, though final confirmation will come at the end of 2006.
Global TB control report: http://www.who.int/tb/publications/global_report/2006/downlo ad_centre/en/index.html
Source: http://www.who.int/mediacentre/news/releases/2006/pr15/en/in dex.html

27. *March 22, Associated Press* — **China turns over bird flu samples.** China agreed to turn over bird flu samples from poultry to the World Health Organization (WHO). The WHO expects to receive about 20 virus samples from China within a few weeks, Julie Hall, an official from the

WHO office in Beijing, said. Experts say such samples are needed to develop diagnostic tools and vaccines, and they have criticized China's Agriculture Ministry for refusing since 2004 to release them to foreign scientists. China's Health Ministry regularly provides samples from human cases of bird flu. China and the WHO reached an agreement after working out "intellectual property rights and issues such as commercial rights," Hall said without giving details.
Source: http://www.chron.com/disp/story.mpl/ap/world/3741415.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

28. *March 22, KTVA (AK)* — **Emergency readiness in Alaska.** The city of Anchorage, AK, unveiled a new program aimed at keeping its residents safer this week. Tuesday, March 21, the mayor along with several representatives from area agencies teamed up to help launch Emergency Watch. The idea behind the program is to arm neighborhoods with leaders, resources and plans in the event of a natural disaster or any other kind of emergency.
Source: http://ktva.com/topstory/ci_3625512

29. *March 22, Oregon Public Broadcasting* — **U.S. Coast Guard exercise simulates terrorist attack.** The Portland Vancouver area U.S. Coast Guard simulated a massive explosion on a fuel−laden barge in the Columbia River Wednesday, March 22. Two hundred people and more than 30 public safety agencies are taking part in the two−day exercise, which is designed to prepare emergency responders for a terrorist attack and environmental disaster. U.S. Coast Guard Petty Officer Amy Gaskill said, "We received a phone call early this morning at our search and rescue station that said that a barge had exploded and there were people in the water that needed assistance." As the disaster unfolded, the Coast Guard set up an operations center on Swan Island. The idea is that whether it's an exercise or a real problem, the lay out is the same and responders know where to go for the information they need.
Source: http://www.publicbroadcasting.net/opb/news.newsmain?action=article&ARTICLE_ID=893127

30. *March 22, Associated Press* — **Texas governor orders hurricane evacuation plan .** Governor Rick Perry ordered state officials on Tuesday, March 21, to develop an improved hurricane evacuation plan to prevent the kind of chaos and gridlock that occurred when millions of Houston−area residents tried to get out ahead of Hurricane Rita last year. Perry’s executive order listed most of the recommendations made by a task force he assigned to develop improved evacuation methods.
Source: http://www.aberdeennews.com/mld/inquirer/news/nation/14156701.htm?source=rss&channel=inquirer_nation

31. *March 21, Kennebec Journal (ME)* — **Bill fleshes out Maine's disaster planning.** A bill designed to make the state of Maine better prepared for terrorist incidents or natural disasters gained support Monday, March 20, from emergency management experts, doctors and firefighters. Members of the Criminal Justice and Public Safety Committee heard near−unanimous support for the bill, which makes organizational changes in state government and works to ensure better communication in emergencies. In addition to putting specific job qualifications in state law, the bill proposes to have the emergency management director report directly to the governor in emergency situations. The bill also proposes to put the Criminal Justice and Public Safety Committee in charge of all state departments that handle homeland security and would require new schools built in the state to be wired for emergency generators.
Source: http://kennebecjournal.mainetoday.com/news/local/2556099.sht ml

32. *March 21, Chillicothe Gazette (OH)* — **Disaster leaves Ohio city to consider emergency plan.** The disaster left by last year's hurricane season has forced many communities to look at their own emergency plans in case any type of disaster should hit close to home. Chillicothe City, OH, Council met with numerous department heads Monday, March 20, to get an understanding of how the city would react in the case of a flood, tornado or pandemic. Chillicothe Fire Chief Bruce Vaughn presented council with a copy of the Ross County Emergency Operations Plan that was developed by the Ross County Emergency Management Agency with representatives from departments throughout the county. The plan includes guidelines for everything that has to be handled during an emergency including communication, evacuation and resource management.
Source: http://www.chillicothegazette.com/apps/pbcs.dll/article?AID=/20060321/NEWS01/603210301/1002

33. *March 19, Mobile Register (AL)* — **Hurricane poll: Worry, readiness high.** Two−thirds of coastal Alabama residents said they believe that this year's hurricane season will be as bad as or worse than last year, and huge numbers have already taken precautions, a new poll indicates. In fact, 43 percent of respondents to the Mobile Register−University of South Alabama poll of Mobile and Baldwin county residents said they own a generator, and another 20 percent said they plan to purchase one before the hurricane season begins June 1. "What you see here is a great deal of anxiety regarding the coming hurricane season," said Keith Nicholls, director of the USA polling group, which conducted the survey last week in Mobile and Baldwin counties. Nicholls and emergency management officials attributed the uneasy feelings to a combination of factors: The 2004 and 2005 seasons brought the destruction of hurricanes Ivan, Katrina and other storms. Of the 400 adults responding to the poll, 85 percent said they had done something to get ready for the coming hurricane season. Overall, emergency management officials said they hoped that residents are following long−standing advice to create an emergency kit and plan for evacuations prior to any storm threats.
Source: http://www.al.com/news/mobileregister/index.ssf?/base/news/114276382750830.xml&coll=3

[Return to top]

Information Technology and Telecommunications Sector

34.

March 22, FrSIRT — **Linux kernel "do_replace" and "NDIS" response buffer overflow vulnerabilities.** Two vulnerabilities have been identified in Linux kernel, which could be exploited by attackers to execute arbitrary commands or cause a denial−of−service. Analysis: The first issue is due to a buffer overflow error in the do_replace() function [Netfilter module], which could be exploited by attackers to cause a kernel memory corruption and possibly execute arbitrary commands with elevated privileges. The second flaw is due to a buffer overflow error in drivers/usb/gadget/rndis.c when processing NDIS responses to OID_GEN_SUPPORTED_LIST, which could be exploited by attackers to cause a memory corruption and possibly execute arbitrary commands with elevated privileges. Affected products: Kernel versions prior to 2.6.16.
Solution: Upgrade to kernel version 2.6.16: http://www.kernel.org/
Source: http://www.frsirt.com/english/advisories/2006/1046

35. *March 22, FrSIRT* — **Motorola Phones buffer overflow and security dialog spoofing vulnerabilities.** Two vulnerabilities have been identified in various Motorola cell phones, which could be exploited by attackers to execute arbitrary commands, bypass security restrictions, and disclose sensitive information. Analysis: The first issue is due to a buffer overflow error when handling an overly long OBEX "setpath()" sent via the OBEX File Transfer service, which could be exploited by an attacker to crash a vulnerable handset or potentially execute arbitrary code via a paired device. The second flaw is due to an input validation error when handling incoming connection to the "Headset Audio Gateway" on Channel 3 from a remote Bluetooth device, which could be exploited by attackers to spoof the device name displayed in security dialogs and convince a user to accept an incoming connection. Affected products: Motorola PEBL U6 and Motorola V600. Solution: The FrSIRT is not aware of any official supplied patch for this issue.
Source: http://www.frsirt.com/english/advisories/2006/1045

36. *March 22, Security Focus* — **Microsoft ASP.NET COM components W3WP remote denial−of−service vulnerability.** Improper access of COM and COM+ components in ASP.NET applications can cause a denial−of−service condition in 'w3wp.exe' processes. Analysis: A remote attacker can exploit this issue to cause denial−of−service conditions in applications using improperly coded ASP.NET, effectively denying service to legitimate users. Vulnerable: Microsoft ASP.NET 1.1 SP1; Microsoft ASP.NET 1.1; Microsoft ASP.NET 1.0 SP2; Microsoft ASP.NET 1.0 SP1; Microsoft ASP.NET 1.0; Microsoft ASP.NET.
Solution details: http://www.securityfocus.com/bid/17188/solution
Source: http://www.securityfocus.com/bid/17188/references

37. *March 22, Hackers Center* — **Trend Micro InterScan Messaging "ISNTSmtp" directory insecure permissions.** A vulnerability has been identified in TrendMicro InterScan Messaging Security Suite, which could be exploited by local attackers to obtain elevated privileges. Analysis: This flaw is due to insecure permissions (Everyone/Full Control) being set on the "ISNTSmtp" directory, which could be exploited by malicious users to delete certain files or replace them with malicious binaries. Affected products: TrendMicro InterScan Messaging Security Suite version 5.5 build 1183 and prior.
Solution: Upgrade to TrendMicro InterScan Messaging Security Suite version 5.7.0.1121: http://www.trendmicro.com/en/products/gateway/ismss/evaluate /overview.htm
Source: http://www.hackerscenter.com/archive/view.asp?id=23774

38. *March 21, Information Week* — **Many data centers still have no risk management plan.** Business technology managers are facing tough challenges as data centers grow larger and more complex. More than 75 percent of all companies have experienced a business disruption in the past five years, including 20 percent who say the disruption had a serious impact on the business, according to a recent survey of data center managers. Despite the critical nature of data center operations to business, nearly 17 percent reported they have no risk management plan, and less than 5 percent have plans that address viruses and security breaches. The results, which were announced Tuesday, March 21, at the Data Center World conference in Atlanta, are part of survey of nearly 200 members of AFCOM, a leading association for data center managers. Some of the predictions: Within the next five years, one out of every four data centers will experience a serious disruption; by 2015, the talent pool of qualified senior−level technical and management data center professionals will shrink by 45 percent; and over the next five years, power failures and limits on power availability will halt data center operations at more than 90 percent of companies.
Source: http://www.securitypipeline.com/news/183701727

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis:

US−CERT is aware of a vulnerability in the way Microsoft Internet Explorer handles the createTextRange() DHTML method. By persuading a user to access a specially crafted webpage, a remote, unauthenticated attacker may be able to execute arbitrary code on that user's system. This vulnerability can also be used to crash Internet Explorer. We are aware of proof of concept code for this vulnerability. More information about the reported vulnerability can be found in VU#876678 − Microsoft Internet Explorer createTextRange() vulnerability
http://www.kb.cert.org/vuls/id/876678

Known attack vectors for this vulnerability require Active Scripting to be enabled in Internet Explorer. Disabling Active Scripting will reduce the chances of exploitation. Until an update, patch or more information becomes available, US−CERT recommends disabling Active Scripting as specified in the Securing Your Web Browser document:
http://www.us−cert.gov/reading_room/securing_browser/#how_to_secure

TSP Phishing Scams: US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. Specifically, sites that provide online benefits are being targeted. Recently, the phishing scam targeted the Thrift Savings Plan (TSP), a retirement savings plan for United States government

employees and members of the uniformed services. For more information please see Thrift Savings Plan (TSP): http://www.tsp.gov/

If you were affected by the TSP phishing scam, please refer to the TSP E−mail scam instructions for assistance: http://www.tsp.gov/curinfo/emailscam.html

US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT: http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online: http://onguardonline.gov/phishing.html

Additionally, users are encouraged to take the following measures to prevent phishing attacks from occurring:

* Do not follow unsolicited web links received in email messages.

* Contact your financial institution immediately if you believe your account and/or financial information has been compromised.

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 6881 (bittorrent), 445 (microsoft−ds), 139 (netbios−ssn), 32459 (−−−), 25 (smtp), 5435 (dttl), 49200 (−−−), 49155 (−−−), 6588 (AnalogX) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.
[Return to top]

General Sector

Nothing to report.
[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer